DERWENT-ACC-NO: 1998-449285

DERWENT-WEEK: 199944

TITLE: Data verification method for postal franking meter imprints - having XOR and encryption functions to generate data authentication code that is imprinted in graphical symbol form

INVENTOR: THIEL, W; WAGNER, A ; WINDEL, H

PATENT-ASSIGNEE: FRANCOTYP-POSTALIA & CO AG[FRANN]

PRIORITY-DATA: 1997US-0798604 (February 11, 1997)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
EP 862143 A2	September 2, 1998	E	054	G07B 017/02
US 5953426 A	September 14, 1999	N/A	000	H04L 009/00

DESIGNATED-STATES: AL AT BE CH DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
EP 862143A2	N/A	1998EP-0250018	January 21, 1998
US 5953426A	N/A	1997US-0798604	February 11, 1997

INT-CL (IPC): G07B017/02, H04L009/00 , H04L009/06

ABSTRACTED-PUB-NO: EP 862143A

BASIC-ABSTRACT:

The method involves dividing data into several data blocks, each containing an equal number of bits. An initialisation vector equal to zero is set. An exclusive-OR operation is conducted with the data blocks to obtain a exclusive-OR result. The exclusive-OR result is encrypted to obtain an output vector. An exclusive-OR operation is conducted with next data blocks and the output vector, as a preceding vector, to obtain a next exclusive-OR result. The result is encrypted to obtain a next output vector.

The steps are repeated in succession for each data block using

the next output vector as the preceding vector to obtain a final output vector containing several bits.

A portion of the bits of the final output vector are selected as a data authentication code for the data. The data are verified using the authentication code.

ADVANTAGE - Provides combination of imprinted security code and remote checks
that avoid undue unannounced inspections.

ABSTRACTED-PUB-NO: US 5953426A

EQUIVALENT-ABSTRACTS:

The method involves dividing data into several data blocks, each containing an equal number of bits. An initialisation vector equal to zero is set. An exclusive-OR operation is conducted with the data blocks to obtain a exclusive-OR result. The exclusive-OR result is encrypted to obtain an output vector. An exclusive-OR operation is conducted with next data blocks and the output vector, as a preceding vector, to obtain a next exclusive-OR result. The result is encrypted to obtain a next output vector.

The steps are repeated in succession for each data block using

the next output vector as the preceding vector to obtain a final output vector containing several bits.

A portion of the bits of the final output vector are selected as a data authentication code for the data. The data are verified using the authentication code.

ADVANTAGE - Provides combination of imprinted security code and remote checks
that avoid undue unannounced inspections.

CHOSEN-DRAWING: Dwg.18/19

TITLE-TERMS: DATA VERIFICATION METHOD POSTAL FRANKING METER IMPRINT
EXCLUSIVE=OR ENCRYPTION FUNCTION GENERATE DATA AUTHENTICITY CODE
IMPRINT GRAPHICAL SYMBOL FORM

DERWENT-CLASS: T01 T04 T05

EPI-CODES: T01-D01; T04-C02; T04-D07C; T05-C05;

SECONDARY-ACC-NO:
Non-CPI Secondary Accession Numbers: N1998-350393